ILLEGAL ACCESS PREVENTION METHOD AND SYSTEM

Patent number: JP10271154
Publication date: 1998-10-09

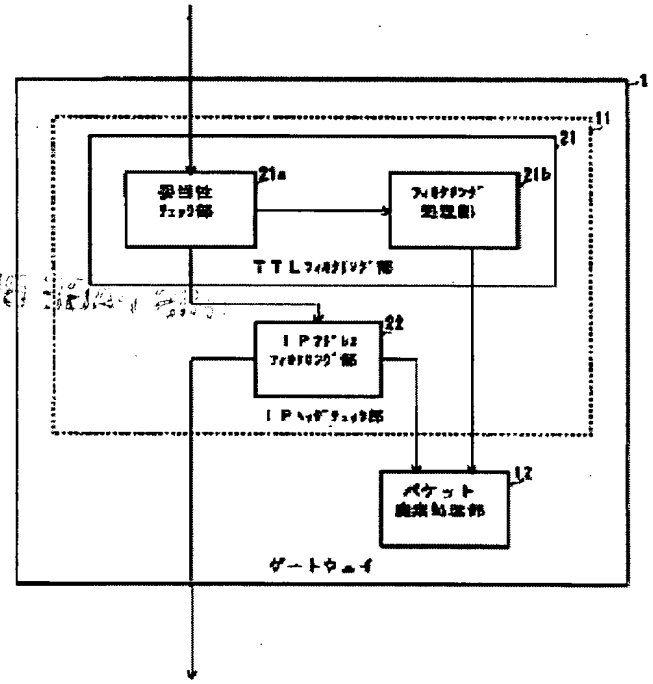
Inventor: MATSUOKA YOSHIE
Applicant: NEC ENG LTD

Classification:
- international: H04L12/46; H04L12/28; H04L9/32; H04L9/36; H04L12/56
- european:
Application number: JP19970067929 19970321
Priority number(s):

Abstract of **JP10271154**

PROBLEM TO BE SOLVED: To exclude an illegal packet by means of filtering utilizing an existing area of a packet without adding an area to a packet data form.

SOLUTION: An IP header check section 11 of a gateway 1 passes only a legal communication packet based on TT (Time To Live: in-network duration time) information and IP address information included in an IP header. A TTL filtering section 21 of the IP header check section 11 passes only a communication packet having valid TTL information in the IP header. A validity check section 21a checks the validity under the condition that the value of the TTL at packet passing is within a range from a predetermined initial value in a group in advance to a (initial value-maximum passing gateway number). The filtering processing section 21b gives a communication packet whose TTL information does not satisfy a prescribed condition to a packet abort processing section 12.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－271154

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]		識別記号	FI	
Ｈ０４Ｌ	12/46		Ｈ０４Ｌ 11/00	３１０Ｃ
	12/28		9/00	６７１
	9/32			６８５
	9/36		11/20	１０２Ｚ
	12/56			

審査請求　未請求　請求項の数10　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－67929

(22)出願日　平成９年(1997)３月21日

(71)出願人　000232047
日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号

(72)発明者　松岡　芳恵
東京都港区芝浦三丁目18番21号　日本電気エンジニアリング株式会社内

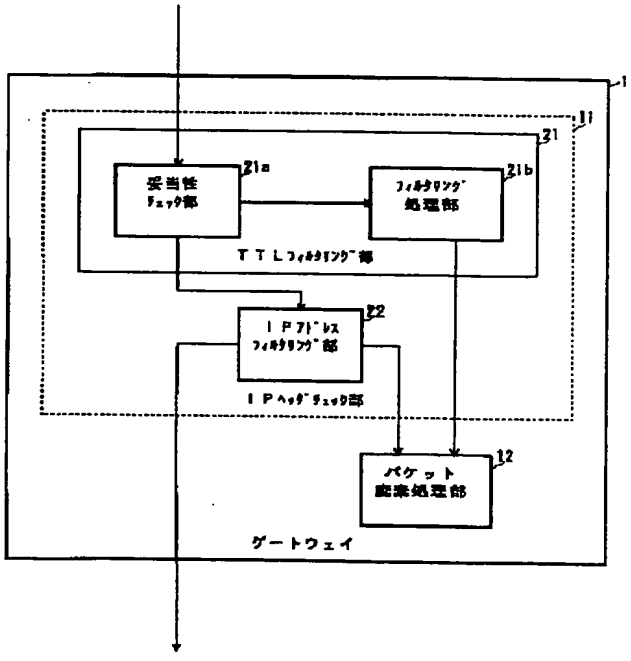
(74)代理人　弁理士　鈴木　正剛

(54)【発明の名称】　不正アクセス防止方法およびシステム

(57)【要約】

【課題】　パケットのデータ形式にエリアの追加を行うことなく、パケットの既存エリアを利用した不正パケットのフィルタリングによる排除を可能とする。

【解決手段】　ゲートウェイ１のＩＰヘッダチェック部１１は、ＩＰヘッダに含まれるＴＴＬ（Time To Live：ネットワーク内存続時間）情報およびＩＰアドレス情報に基づいて、不正でない通信パケットのみを通過させる。ＩＰヘッダチェック部１１のＴＴＬフィルタリング部２１は、ＩＰヘッダ中に妥当性のあるＴＴＬ情報を有する通信パケットのみを通過させる。妥当性チェック部２１ａは、パケット通過時のＴＴＬの値が、予めグループ内で取り決めた初期値から（初期値－最大通過ゲートウェイ数）までの範囲内であることを条件として妥当性をチェックする。フィルタリング処理部２１ｂはＴＴＬ情報が所定の条件を満足していない通信パケットをパケット廃棄処理部１２に与える。



【特許請求の範囲】

【請求項１】　複数の支線ネットワークが結合装置により結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークにおいて、該論理グループにおける不正アクセスを防止するにあたり、

送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定めておき、

前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行うようにした、ことを特徴とする不正アクセス防止方法。

【請求項２】　前記ネットワーク内存続時間情報は、前記結合装置の通過毎に減算される情報を含み、且つ前記機密情報としてのネットワーク内存続時間情報の初期値は、ネットワーク構成に基づいて予想される前記結合装置の最大通過数を超える値に設定するとともに、前記ネットワーク内存続時間情報の値が、前記初期値乃至前記初期値－前記最大通過数の範囲外である場合に前記結合装置が当該パケットを不正パケットと判断することを特徴とする請求項１に記載の不正アクセス防止方法。

【請求項３】　ＩＰ（インターネットプロトコル）アドレスに基づくフィルタリングをさらに併用することを特徴とする請求項１または２に記載の不正アクセス防止方法。

【請求項４】　ＭＡＣ（メディアアクセス制御）アドレスに基づくフィルタリングをさらに併用することを特徴とする請求項１乃至３のうちのいずれか１項に記載の不正アクセス防止方法。

【請求項５】　前記不正パケットは、前記結合装置が廃棄することを特徴とする請求項１乃至４のうちのいずれか１項に記載の不正アクセス防止方法。

【請求項６】　複数の支線ネットワークが結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークシステムにおいて、

前記支線ネットワークに結合され、通信パケットの送信時に、該通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に設定するネットワーク内存続時間情報設定手段を有する端末装置と、

前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックする妥当性チェック手段、および該妥当性チェック手段のチェック結果に基づいて、前記論理グループの内外間での通過パケットをフィルタリングするフィルタリング処理手段を有し、前記複数の支線ネットワークを結合するとともに、該論理グループにおける不正アクセスを防止するネットワーク結合手段

と、を具備することを特徴とする不正アクセス防止システム。

【請求項７】　前記ネットワーク内存続時間情報は、前記ネットワーク結合手段の通過毎に減算される情報を含み、且つネットワーク内存続時間設定手段は、前記機密情報としてのネットワーク内存続時間情報の初期値を、ネットワーク構成に基づいて予想される前記ネットワーク結合手段の最大通過数を超える値に設定する手段を含むとともに、前記妥当性チェック手段は、前記ネットワーク内存続時間情報の値が、前記初期値乃至前記初期値－前記最大通過数の範囲外である場合に当該パケットを不正パケットと判断する手段を含むことを特徴とする請求項６に記載の不正アクセス防止システム。

【請求項８】　前記ネットワーク結合手段は、ＩＰ（インターネットプロトコル）アドレスに基づくフィルタリングを行うＩＰアドレスフィルタリング手段をさらに含むことを特徴とする請求項６または７に記載の不正アクセス防止システム。

【請求項９】　前記ネットワーク結合手段は、ＭＡＣ（メディアアクセス制御）アドレスに基づくフィルタリングを行うＭＡＣアドレスフィルタリング手段をさらに含むことを特徴とする請求項６乃至８のうちのいずれか１項に記載の不正アクセス防止システム。

【請求項１０】　前記ネットワーク結合手段は、フィルタリングによって通過が阻止された不正パケットを廃棄するパケット廃棄手段を含むことを特徴とする請求項６乃至９のうちのいずれか１項に記載の不正アクセス防止システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、通信ネットワークシステムを構築するルータおよびゲートウェイ等における不正アクセスの防止に係り、特に、通信プロトコルとしてＴＣＰ／ＩＰ（Transmission Control Protocol / Internet Protocol：転送制御プロトコル／インターネットプロトコル）を使用している通信ネットワークシステムに好適な不正アクセス防止システムに関する。

【０００２】

【従来の技術】通信ネットワークシステム、例えばＬＡＮ（Local Area Network：ローカルエリアネットワーク）システムは、ルータおよびゲートウェイの少なくともいずれかを介して複数の支線ＬＡＮが接続されて構築されている。このような通信ネットワークシステムにおいて、通信プロトコルとしてＴＣＰ／ＩＰを使用していることも多い。

【０００３】ところで、物理的に接続されているネットワーク上で、必要に応じて論理的にグループ分けを行っている場合がある。このような場合、論理的なグループ内での通信が主体となって、他のグループとの間の通信を、必要としなかったり、排除したりしたいことがあ

る。

【０００４】このような場合には、支線ＬＡＮを接続するルータおよびゲートウェイ等において、パケットのＭＡＣ（Media Access Control：メディアアクセス制御）アドレスまたはＩＰ（Internet Protocol：インターネットプロトコル）アドレスを識別し、他のグループのパケットを通過させないようにして、同報パケット、異常パケット、あるいは不正に他のグループの端末にアクセスしようとするパケット等の不正アクセスパケットの流入および流出を防止することが行われている。

【０００５】このように、パケットのＭＡＣアドレスまたはＩＰアドレスを識別して他のグループのパケットは通過させないようにする機能は、ＭＡＣアドレスによりフィルタリングを行うＭＡＣアドレスフィルタリング機能またはＩＰアドレスによりフィルタリングを行うＩＰアドレスフィルタリング機能と称される。

【０００６】すなわち、ＭＡＣアドレスまたはＩＰアドレスによるフィルタリングは、次のようにして行われる。予め通過を許容するＭＡＣアドレスまたはＩＰアドレスを、ルータあるいはゲートウェイに登録しておく。ルータあるいはゲートウェイは、受信したパケットのＭＡＣアドレスまたはＩＰアドレスと登録されているＭＡＣアドレスまたはＩＰアドレスとを照合して、正しいＭＡＣアドレスまたはＩＰアドレスのパケットのみを通過させる。このようにして、不正アクセスパケットの通過がルータあるいはゲートウェイにより阻止される。

【０００７】ＭＡＣアドレスは、多くの場合端末装置（以下、単に「端末」と称する）に物理的に設定されており、安易に変更することができないことが多い。ところが、ＭＡＣ層アドレスには、全ネットワークに同報パケットを通過させるための同報アドレスが存在するため、同報パケットとの混同が生じる。これを防止するために、ＭＡＣ層よりも上位層であるネットワーク層のＩＰアドレスでフィルタリングするＩＰアドレスフィルタリングが用いられる。

【０００８】しかしながら、ＩＰアドレスは、ＴＣＰ／ＩＰプロトコルに必要なものであり、装置に論理的に設定しているため、比較的容易に変更することが可能である。そのため、グループ外の端末が、当該グループ内の端末のＩＰアドレスを不正に設定してグループ内のＬＡＮシステムに入り込もうとした場合には、ＩＰアドレスのフィルタリングでは、不正アクセスパケットを確実に検出することができない。

【０００９】これに対して、特開平７－１７０２７９号公報には、ＩＰアドレスフィルタリングを用いることなく、不正アクセスパケットを排除する技術が開示されている。

【００１０】すなわち、特開平７－１７０２７９号公報に示されたシステムは、ＭＡＣアドレスによるフィルタリングを行う複数の支線ＬＡＮを収容する従来のブリッ

ジ回路に対して、支線ＬＡＮのグループ番号を登録する機能、パケット送信時に該グループ番号をパケットに付加する機能、およびパケットに付加されたグループ番号と登録されたグループ番号とをパケット受信時に照合する機能を付加したブリッジ回路を用いる。

【００１１】このブリッジ回路に収容したＬＡＮそれぞれにグループ番号を設定し、同一グループ内のＬＡＮ間転送時には基幹バスへ送信するパケットに、該グループ番号を付加する。基幹バスからパケットを受信するときはブリッジ回路が元来行っていたフィルタリング機能であるＭＡＣアドレスによるフィルタリングを行う前に、送信時にパケットに付加されたグループ番号によるフィルタリングを行う。

【００１２】すなわち、複数の端末が接続される複数の支線ＬＡＮを複数のブリッジ回路を介して基幹バスに接続するシステムにおいて、複数のブリッジ回路に個々に収容された複数の支線ＬＡＮを独立した複数のグループにグループ化し、各ブリッジ回路にはそれぞれ収容する支線ＬＡＮのグループ番号を予め登録しておく。端末から同一グループ内の他の支線ＬＡＮへ送信するパケットには、ブリッジ回路は、該端末が属する支線ＬＡＮのグループ番号を付加して基幹バスに送信する。基幹バスを介してパケットを受信したときには、ブリッジ回路は、受信したパケットに付加されているグループ番号を識別し、登録されている番号と照合して、両者が一致したときにのみ、この受信したパケットに対してＭＡＣアドレスフィルタリング機能を動作させブリッジ回路が収容している支線ＬＡＮに送信する。

【００１３】このようにすることにより、ＬＡＮのＭＡＣ層における同報パケット、異常パケットまたは不正に他のグループの端末に他のグループの端末と通信しようとするパケット等の不正アクセスパケットを、グループ番号の相違により阻止することができる。

【００１４】

【発明が解決しようとする課題】上述したように、特開平７－１７０２７９号公報に示されたシステムは、ブリッジ回路に収容した複数のＬＡＮにそれぞれグループ番号を設定し、同一グループ内のＬＡＮ間転送時には基幹バスへ送信するパケットに、該グループ番号を付加する。基幹バスからパケットを受信するときはブリッジ回路が元来行っていたフィルタリング機能であるＭＡＣアドレスによるフィルタリングを行う前に、送信時にパケットに付加されたグループ番号によるフィルタリングを行う。

【００１５】この特開平７－１７０２７９号公報のシステムによれば、グループ番号の相違をチェックすることにより、ＬＡＮのＭＡＣ層における同報パケット、異常パケットまたは不正に他のグループの端末に他のグループの端末と通信しようとするパケット等の不正アクセスパケットを阻止することができる。

【００１６】しかしながら、特開平７－１７０２７９号公報に示された、ブリッジ回路にグループ番号を登録し、送信パケットにこのグループ番号を付加して、パケットを受信したときに受信パケットのグループ番号と登録したグループ番号の照合を行うフィルタリングを可能とするためには、パケットのデータ形式にグループ番号エリアを追加する必要がある。

【００１７】ところが、ＬＡＮのパケットには、物理層のヘッダ部およびトランスポート層のヘッダ部等が含まれており、パケットのデータ形式が細かく規定されていることが多い。したがって、パケットのデータ形式が規定されているＬＡＮシステムにおいては、多くの場合、在来のパケットにグループ番号を格納するためのエリアを追加して確保することができず、特開平７－１７０２７９号公報に記載された技術を実施することができない。

【００１８】この発明は、上述した事情に鑑みてなされたもので、パケットの既存エリアを利用した不正パケットのフィルタリングを可能とし、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除を可能とする不正アクセス防止方法およびシステムを提供することを目的とする。

【００１９】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係る不正アクセス防止方法は、複数の支線ネットワークが結合装置により結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークにおいて、該論理グループにおける不正アクセスを防止するにあたり、送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定めておき、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行うようにする。

【００２０】前記ネットワーク内存続時間情報は、前記結合装置の通過毎に減算される情報を含み、且つ前記機密情報としてのネットワーク内存続時間情報の初期値は、ネットワーク構成に基づいて予想される前記結合装置の最大通過数を超える値に設定するとともに、前記ネットワーク内存続時間情報の値が、前記初期値乃至前記初期値－前記最大通過数の範囲外である場合に前記結合装置が当該パケットを不正パケットと判断するようにしてもよい。

【００２１】前記不正アクセス防止方法は、さらに、ＩＰアドレスに基づくフィルタリングをさらに併用するようにしてもよい。

【００２２】前記不正アクセス防止方法は、さらに、ＭＡＣアドレスに基づくフィルタリングをさらに併用するようにしてもよい。

【００２３】前記不正アクセス防止方法は、前記不正パケットを、前記結合装置が廃棄するようにしてもよい。

【００２４】この発明の第２の観点に係る不正アクセス防止システムは、複数の支線ネットワークが結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークシステムにおいて、前記支線ネットワークに結合され、通信パケットの送信時に、該通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に設定するネットワーク内存続時間情報設定手段を有する端末装置と、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックする妥当性チェック手段、および該妥当性チェック手段のチェック結果に基づいて、前記論理グループの内外間での通過パケットをフィルタリングするフィルタリング処理手段を有し、前記複数の支線ネットワークを結合するとともに、該論理グループにおける不正アクセスを防止するネットワーク結合手段と、を具備する。

【００２５】前記ネットワーク内存続時間情報は、前記ネットワーク結合手段の通過毎に減算される情報を含み、且つネットワーク内存続時間設定手段は、前記機密情報としてのネットワーク内存続時間情報の初期値を、ネットワーク構成に基づいて予想される前記ネットワーク結合手段の最大通過数を超える値に設定する手段を含むとともに、前記妥当性チェック手段は、前記ネットワーク内存続時間情報の値が、前記初期値乃至前記初期値－前記最大通過数の範囲外である場合に当該パケットを不正パケットと判断する手段を含んでいてもよい。

【００２６】前記ネットワーク結合手段は、ＩＰアドレスに基づくフィルタリングを行うＩＰアドレスフィルタリング手段をさらに含んでいてもよい。

【００２７】前記ネットワーク結合手段は、ＭＡＣアドレスに基づくフィルタリングを行うＭＡＣアドレスフィルタリング手段をさらに含んでいてもよい。

【００２８】前記ネットワーク結合手段は、フィルタリングによって通過が阻止された不正パケットを廃棄するパケット廃棄手段を含んでいてもよい。

【００２９】この発明の不正アクセス防止方法およびシステムにおいては、複数の支線ネットワークが結合装置により結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークの該論理グループにおける不正アクセスを防止するために、送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定め、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリン

グを行う。したがって、パケットの既存エリアであるネットワーク内存続時間情報を利用して不正パケットのフィルタリングを行うことができ、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除が可能となる。

【００３０】

【発明の実施の形態】以下、この発明の実施の形態を図面を参照して説明する。

【００３１】この発明の実施の形態に係る不正アクセス防止システムは、ＴＣＰ／ＩＰプロトコルを用いた通信ネットワークシステムに適用している。この実施の形態では、ＴＣＰ／ＩＰプロトコルのＩＰヘッダ内の既存のエリアであるＴＴＬを利用することにより不正パケットのフィルタリングを行うことにより、通信パケットの在来のデータ形式のままで不正アクセスを効果的に防止する。

【００３２】ＴＣＰ／ＩＰプロトコルによる通信パケットのＩＰヘッダには、ＴＴＬ（Timeto Live：ネットワーク内存続時間）情報を格納するためのＴＴＬエリアが設けられている。ＴＴＬ情報とは、通信パケットが、あとどれだけの時間ネットワーク内に存続できるか、すなわち存続残時間を秒単位で示したものである。この存続算時間は、秒単位を基本としているが、処理時間が１秒に満たない場合および処理時間が計測できない場合があり、一般に、例えばルータまたはゲートウェイのような結合装置を通過する度に、その都度“１”マイナスされ、このＴＴＬの値が“０”である通信パケットを検出したときに、その通信パケットは、存続時間が満了したものとして廃棄される。このようなＴＴＬ情報は、永遠に配達されずに、ネットワーク中を浮遊するパケットが発生することを防止するために設けられている。ＴＣＰ／ＩＰプロトコルにおいては、ＴＴＬの最大値は“２５５（秒）”である。一般には、送信端末から受信端末までのルータおよびゲートウェイ等の結合装置の数は、不達パケットの発生を防止するために多めに見積もられる。しかも、このＴＴＬの値は、仮に最大値を設定しても送信から２５５秒たった時点で通信パケットが廃棄されるため、通常の場合、かなり大きめに設定される。

【００３３】この発明では、論理的なグループ内で、ＴＴＬの初期値を機密情報として予め取り決めておき、グループ内の送信端末から受信端末までにパケットが通過すると予想されるルータおよびゲートウェイ等の結合装置の最大数を設定しておく。この結合装置の最大数よりも、ＴＴＬの初期値を大きく設定しておく。パケットのフィルタリングにあたっては、パケット通過時のＴＴＬの値がＴＴＬの初期値から（初期値－最大通過結合装置数）までの範囲であれば正常パケット、該範囲外であれば不正パケットと判断する。

【００３４】このような仕組みにより、グループ内の端末のＩＰアドレスを使用して不正にグループ内の端末に

アクセスしようとするグループ外の不正な端末からの不正パケットを排除することができる。

【００３５】図１～図３を参照して、上述した原理に基づくこの発明による不正アクセス防止システムを組み込んだネットワークシステムの実施の形態を説明する。

【００３６】図１は、この発明の実施の形態に係る不正アクセス防止システムを組み込んだゲートウェイの主要部の構成を示している。

【００３７】図１に示すゲートウェイ１は、ＩＰヘッダチェック部１１およびパケット廃棄処理部１２を具備している。

【００３８】ＩＰヘッダチェック部１１は、ＩＰヘッダの情報をチェックし、ＩＰヘッダに含まれるＴＴＬ（Time to Live：ネットワーク内存続時間）情報およびＩＰアドレス情報に基づいて、当該論理グループの内部から外部へ、および外部から内部への通過パケットをチェックして、不正でない通信パケットのみを通過させ、不正パケットの通過を阻止する。パケット廃棄処理部１２は、ＩＰヘッダチェック部１１により、通過が阻止された不正パケットを廃棄処理する。

【００３９】ＩＰヘッダチェック部１１は、ＴＴＬフィルタリング部２１およびＩＰアドレスフィルタリング部２２を有する。

【００４０】ＴＴＬフィルタリング部２１は、妥当性チェック部２１ａおよびフィルタリング処理部２１ｂを有し、ＩＰヘッダ中のＴＴＬ情報の妥当性をチェックして、ＴＴＬ情報として妥当性のあるＴＴＬ情報を有する通信パケットのみを通過させ、妥当性のないＴＴＬ情報を有する通信パケットの通過を阻止する。

【００４１】妥当性チェック部２１ａは、通信パケットの通過時にＩＰヘッダにおけるＴＴＬ情報が所定の条件を満足しているか否かに基づいて、ＴＴＬ情報の妥当性をチェックする。フィルタリング処理部２１ｂは、論理グループの内外間での通過パケットに対し、妥当性チェック部２１ａのチェック結果に基づいて、ＴＴＬ情報が所定の条件を満足している通信パケットのみを通過させ、該所定の条件を満足していない通信パケットをパケット廃棄処理部１２に与える。

【００４２】上述したようにゲートウェイ１におけるＴＴＬ情報を用いたフィルタリングでは、各論理グループにおいて、予めグループ内でのＴＴＬの初期値を機密データとして取り決め、且つグループ内の送信端末から受信端末までにパケットが通過する結合装置、例えばゲートウェイおよびルータ等、の最大数を設定しておく。そして、これらＴＴＬの初期値と最大通過結合装置数をゲートウェイ１の妥当性チェック部２１ａに予め登録しておくことにより、妥当性チェック部２１ａは、パケット通過時のＴＴＬの値がＴＴＬの初期値から（初期値－最大通過ゲートウェイ数）までの範囲内であるか否かを条件として妥当性をチェックする。ＴＴＬの値が該範囲内

であれば正常パケットすなわち妥当性ありと判定し、当該範囲外であれば不正パケットすなわち妥当性なしと判定する。

【００４３】ＩＰアドレスフィルタリング部２２は、ＩＰヘッダにおけるＩＰアドレス情報に基づいて、当該論理グループの外部から該論理グループの内部のアドレスへの通信パケットおよび当該論理グループの内部から該論理グループの外部のアドレスへの通信パケットを通過させ、それ以外のＩＰアドレス情報を有する通信パケットの通過を阻止してパケット廃棄処理部１２に与える。

【００４４】図１に示したゲートウェイ１を用いて構成したネットワークシステムを図２に示す。図２においては、在来のフィルタリング機能を有するゲートウェイと図１のこの発明によるフィルタリング機能を有するゲートウェイとを用いて不正アクセス防止システムを構成している。

【００４５】図２に示すネットワークシステムは、第１のゲートウェイ１、第２のゲートウェイ２、第１の端末３、第２の端末４、第３の端末５、第１の支線ＬＡＮ６、第２の支線ＬＡＮ７および第３の支線ＬＡＮ８を備えている。第１の端末３および第２の端末４は、第１の支線ＬＡＮ６に結合されており、第３の端末５は第３の支線ＬＡＮ８に結合されている。第１の支線ＬＡＮ６と第２の支線ＬＡＮ７とは第２のゲートウェイ２により結合されており、第２の支線ＬＡＮ７と第３の支線ＬＡＮ８とは第２のゲートウェイ１により結合されている。

【００４６】第１および第２のゲートウェイ１および２は、それぞれ第２の支線ＬＡＮ７と第３の支線ＬＡＮ８との間、および第１の支線ＬＡＮ６と第２の支線ＬＡＮ７との間で通信パケット等のデータを転送する。

【００４７】第１のゲートウェイ１は、図１に示したこの発明に基づく通信パケットのフィルタリング機能を有するゲートウェイである。すなわち、第１のゲートウェイ１は、この発明によるＴＴＬ情報を用いた通信パケットのフィルタリング機能と、在来のＩＰアドレスを用いた通信パケットのフィルタリング機能とを有している。

【００４８】第２のゲートウェイは、在来のゲートウェイであり、ＩＰアドレスを用いた通信パケットのフィルタリング機能のみを有している。

【００４９】第２の端末４および第３の端末５が同一グループを構成し、第１の端末３はグループ外の端末であるとする。

【００５０】この場合、例えば、端末４と端末５とで構成されるグループ内では、機密データとしてＴＴＬの初期値を“５”と設定しているものとする。また、最大通過結合装置数、すなわち最大通過ゲートウェイ数は、ゲートウェイ１および２が存在するため“２”である。これらの値は、ゲートウェイ１の妥当性チェック部２１ａに予め設定される。

【００５１】グループ外の端末３は、端末４と端末５とのグループ間で取り決めたＴＴＬの初期値がわからないため、端末３では、ＴＴＬの初期値を“３２”と設定したものとする。端末４が端末５に通信パケットを送信したときの動作、および端末４が支線ＬＡＮ６に接続していない状態で端末３が端末４を装って、端末４のＩＰアドレスに設定して、端末５に不正にアクセスしようとした場合の動作について、図３に示すフローチャートを参照して説明する。図３に示すフローチャートは、図１のゲートウェイ１のＩＰヘッダチェック部１１におけるＩＰヘッダのチェック処理の流れを示している。

【００５２】ゲートウェイ２にはＩＰアドレスのフィルタリングのみを行うために端末４と端末５のＩＰアドレスを登録する。ゲートウェイ１には、ＩＰアドレスのフィルタリングのために端末４と端末５のＩＰアドレスを登録し、且つＴＴＬによるフィルタリングのために、端末４と端末５との間で取り決めたＴＴＬの初期値α“５”と最大通過ゲートウェイ数“２”とを内部の妥当性チェック部２１ａに記憶させる。

【００５３】まず、端末４が同一グループ内の端末５に通信パケットを送信する場合の動作について説明する。

【００５４】端末４は、自分のＩＰアドレス、つまり発信元ＩＰアドレス、に端末４のＩＰアドレスを設定し、相手のＩＰアドレス、つまり宛先（送信先）ＩＰアドレスに相手先端末５のＩＰアドレスを設定するとともに、ＴＴＬには当該グループ間で取り決めた初期値α“５”をセットして、通信パケットを支線ＬＡＮ６に送信する。

【００５５】送信されたパケットは、ゲートウェイ２で受信される。ゲートウェイ２は、ＩＰヘッダをチェックする。ゲートウェイ２は、発信元ＩＰアドレスが登録されている端末４のアドレスであり、宛先ＩＰアドレスが登録されている端末５のアドレスであるため、正常パケットとみなす。正常パケットとみなすと、ゲートウェイ２は、元のＴＴＬ値である“５”から“１”をマイナスした“４”を新たなＴＴＬ値としてＴＴＬにセットして、通信パケットを支線ＬＡＮ７に送信する。

【００５６】支線ＬＡＮ７に送信されたパケットは、さらにゲートウェイ１で受信される。ゲートウェイ１は、ＩＰヘッダチェック部１１において、図３に示すフローチャートに従ってＩＰヘッダのチェックを行う。

【００５７】ＩＰヘッダのチェックが開始されると、ＩＰのバージョンのチェックを行い（ステップＳ１１）、バージョンが異常である場合は、パケット廃棄処理部１２でパケットを廃棄する（ステップＳ１７）。ステップＳ１１で、バージョンが正常であった場合は、ＩＰヘッダのその他の情報のチェックを行い（ステップＳ１２）、該その他の情報の異常を検知した場合にもステップＳ１７に移行してパケットを廃棄する。

【００５８】ステップＳ１２で正常であった場合には、ＴＴＬの値が“０”であるか否かのチェックを行う（ス

テップＳ１３）。ステップＳ１３において、ＴＴＬの値が“０”である場合には、ＴＴＬすなわちネットワーク内存続時間が満了しているので、ステップＳ１７でパケットを廃棄する。この場合には、ＴＴＬの値は、“４”であるので、ステップＳ１３では正常と判定され、ＴＴＬフィルタリング部２１の妥当性チェック部２１ａでＴＴＬの値の妥当性のチェックを行う（ステップＳ１４）。

【００５９】妥当性のチェックは、ＴＴＬの値が初期値α以下で且つ（初期値－最大ゲート数）βを超えているか否かにより行う。ＴＴＬの値がこの範囲内であれば妥当であるとみなす。

【００６０】この場合、初期値αは“５”、（初期値－最大ゲート数）βは“３”（＝５－２）であり、受信したパケットのＴＴＬの値は“４”であるため、正常とみなされる。ステップＳ１４で正常とみなされると、ＩＰアドレスフィルタリング部１２によりＩＰアドレスのチェックを行う（ステップＳ１５）。ステップＳ１４で不正とみなされた場合には、ステップＳ１７でパケットを廃棄する。

【００６１】受信した通信パケットの発信元ＩＰアドレスは登録されている端末４のＩＰアドレスであり、宛先ＩＰアドレスは登録されている端末５のアドレスであるため、正常パケットとみなし、通信パケットは、ゲートウェイ１に受信される（ステップＳ１６）。ゲートウェイ１は、受信したパケットのＴＴＬに“４”から“１”をマイナスした“３”をセットして、通信パケットを支線ＬＡＮ８に送信する。送信された通信パケットは相手先端末である端末５で受信される。

【００６２】次に、端末４が支線ＬＡＮ６に接続されていない状態で、当該グループ外の端末３が端末４を装って不正に端末５にパケットを送信しようとした場合の動作を説明する。

【００６３】端末３は、発信元ＩＰアドレスに端末４のＩＰアドレスを設定し、宛先ＩＰアドレスに相手先端末５のＩＰアドレスを設定して、通信パケットを支線ＬＡＮ６に送信する。しかしこの場合、端末３では、相手先端末５が属する論理グループに属していないので、当該グループ内で取り決めたＴＴＬの初期値がわからない。そのため、端末３は、適当な値として“３２”をＴＴＬにセットして通信パケットを送信する。

【００６４】送信された通信パケットはゲートウェイ２に受信される。ゲートウェイ２は、ＩＰアドレスのフィルタリングのためのＩＰヘッダのチェックを行うが、発信元ＩＰアドレスが登録されている端末４のアドレスであり、宛先ＩＰアドレスが登録されている端末５のアドレスであるため、ＩＰアドレスは正常であるとみなす。そこで、ゲートウェイ２は、“３２”から“１”をマイナスした“３１”をＴＴＬにセットして、該通信パケットを支線ＬＡＮ７に送信する。

【００６５】支線ＬＡＮ７に送信されたパケットはゲートウェイ１で受信される。ゲートウェイ１は、ＩＰヘッダチェック部１１において、図３に示すフローチャートに従ってＩＰヘッダのチェックを行う。

【００６６】ＩＰヘッダのチェックが開始されると、ステップＳ１１でＩＰのバージョンのチェックを行い、バージョンが異常である場合は、ステップＳ１７に移行しパケット廃棄処理部１２でパケットを廃棄する。ステップＳ１１で、バージョンが正常であった場合は、ステップＳ１２で、ＩＰヘッダのその他の情報のチェックを行い、異常を検知した場合には、ステップＳ１７でパケットを廃棄する。

【００６７】ステップＳ１２で、ＩＰヘッダのその他の情報が正常であった場合には、ステップＳ１３で、ＴＴＬの値が“０”であるか否かのチェックを行う。ステップＳ１３のチェックにおいて、もしもＴＴＬの値が“０”であればパケットを廃棄するが、この場合は、ＴＴＬの値が“３１”であるため、ステップＳ１３では正常と判定され、ステップＳ１４でＴＴＬの値の妥当性のチェックを行う。

【００６８】ステップＳ１４の妥当性のチェックにおいて、先に述べたように初期値αは“５”であり、（初期値－最大通過ゲートウェイ数）であるβは“３”（＝５－２）であるが、受信した通信パケットのＴＴＬの値は“３１”であるため、異常とみなされ、ステップＳ１７に移行して、該通信パケットは廃棄される。

【００６９】上述したように、ＩＰヘッダ部分におけるＴＴＬを利用したフィルタリング機能により、ＩＰアドレスフィルタリングでは検出することができない不正パケットを検出し、廃棄して、端末の不正アクセス防止機能の信頼性を向上することができる。

【００７０】なお、図１～図３で説明したこの発明の実施の形態においては、ＴＴＬ情報を利用したフィルタリングに、ＩＰアドレスによるフィルタリングを併用するものとしたが、さらにＭＡＣアドレスに基づくフィルタリング処理を行う手段を設けて、ＭＡＣアドレスフィルタリング機能を併用するようにしてもよい。

【００７１】

【発明の効果】以上説明したように、この発明の不正アクセス防止方法およびシステムにおいては、複数の支線ネットワークが結合装置により結合されたネットワーク内に１以上の論理グループが構成されている通信ネットワークの該論理グループにおける不正アクセスを防止するために、送信時の通信パケットに含まれるネットワーク内存続時間情報の初期値を、予め通信ネットワーク内に設定した論理グループ内における機密情報として、所定値に定め、前記結合装置が、前記通信パケットの通過時に前記ネットワーク内存続時間情報の妥当性をチェックすることにより、前記論理グループの内外間での通過パケットのフィルタリングを行う。したがって、パケッ

13

トの既存エリアであるネットワーク内存続時間情報を利用して不正パケットのフィルタリングを行うことができる。

【００７２】すなわち、この発明によれば、パケットの既存エリアを利用した不正パケットのフィルタリングを可能とし、パケットのデータ形式にエリアの追加を行うことなく、不正パケットの効果的な排除を可能とする不正アクセス防止方法およびシステムを提供することができる。

【図面の簡単な説明】

【図１】この発明の実施の形態に係る不正アクセス防止システムを組み込んだゲートウェイの主要部の構成を示すブロック図である。

【図２】図１のゲートウェイを用いたネットワークシステムの構成を示すブロック図である。

14

【図３】図１のシステムの動作を説明するため、ゲートウェイのＩＰヘッダチェック部におけるＩＰヘッダのチェックの流れを示すフローチャートである。

【符号の説明】

１，２　ゲートウェイ

３～５　端末（端末装置）

６～８　支線ＬＡＮ（Local Area Network）

１１　ＩＰ（Internet Protocol）ヘッダチェック部

１２　パケット廃棄処理部

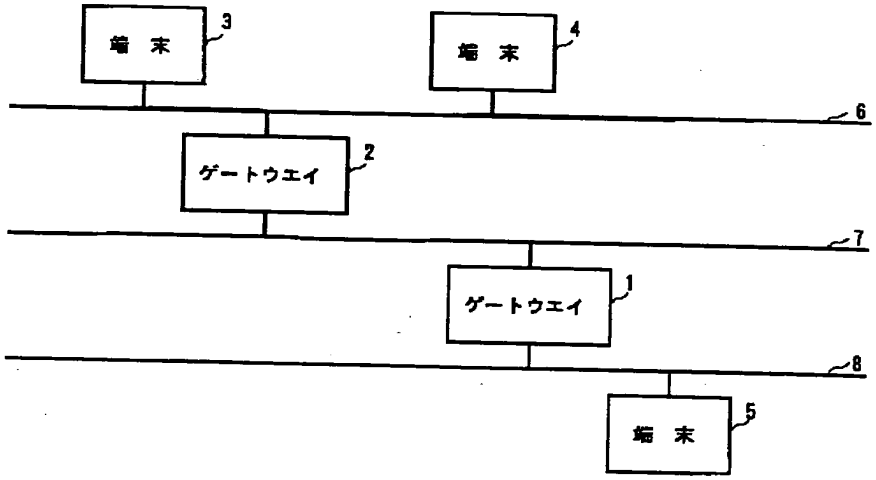
２１　ＴＴＬ（Time to Live）フィルタリング部

２１ａ　妥当性チェック部

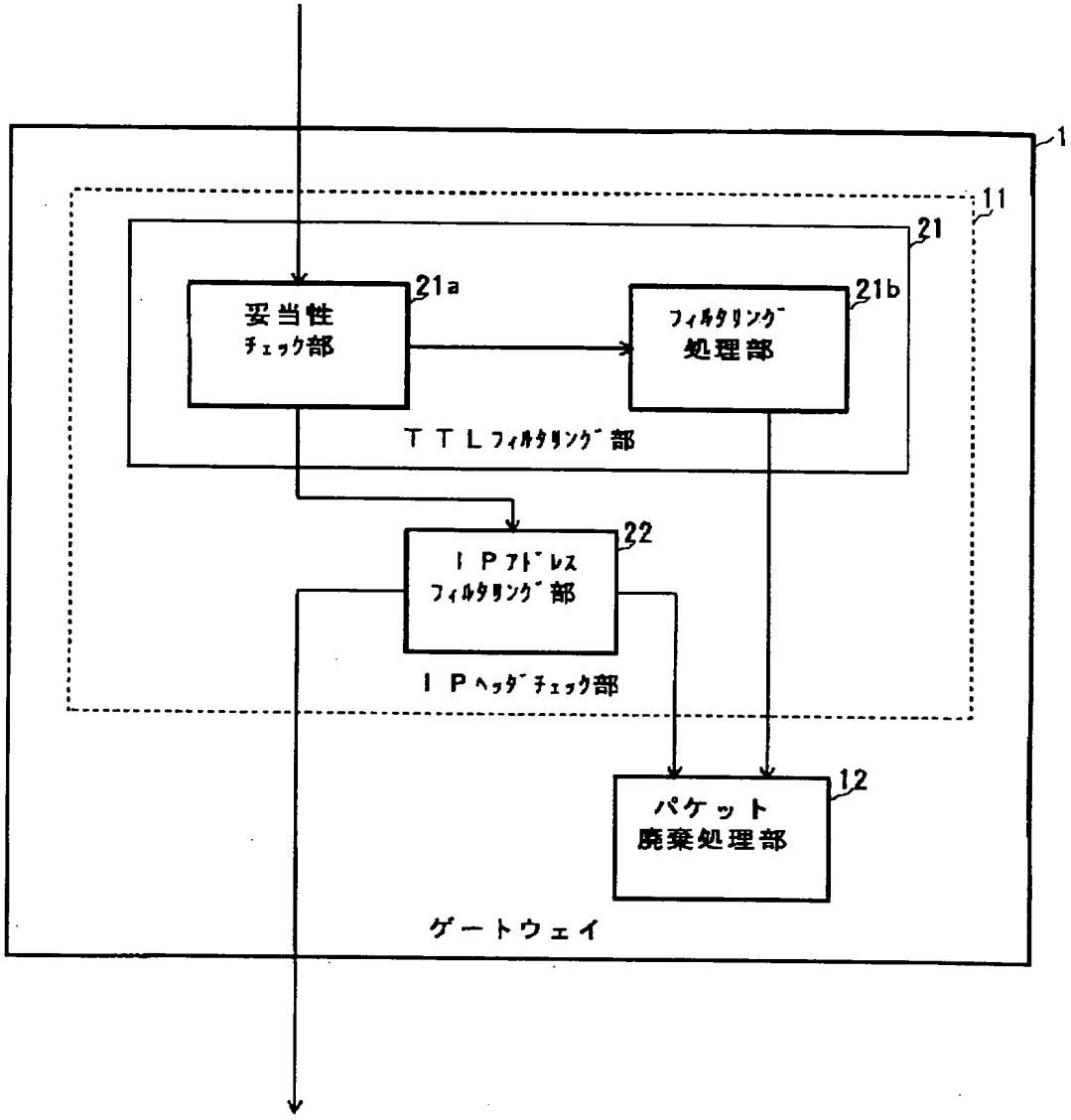
２１ｂ　フィルタリング処理部

２２　ＩＰアドレスフィルタリング部

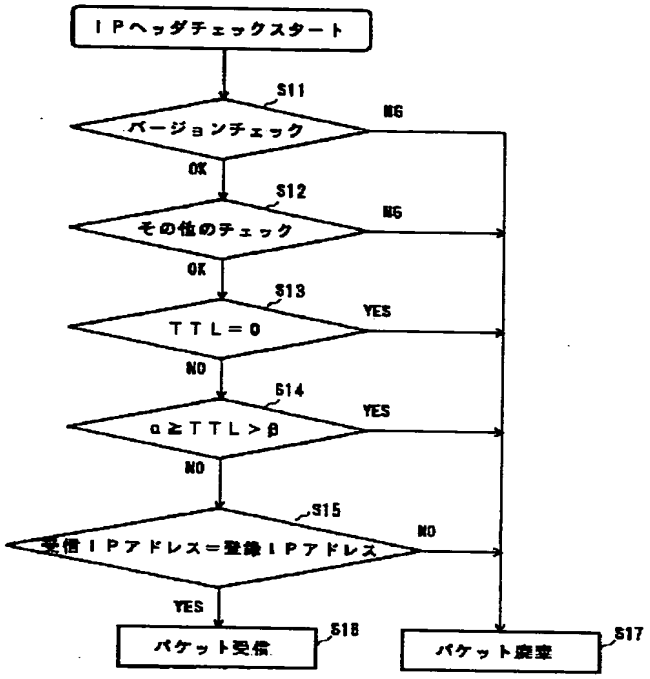
【図２】



【図1】


1
11
21
21a
妥当性
チェック部
21b
フィルタリング
処理部
ＴＴＬフィルタリング部
22
ＩＰアドレス
フィルタリング部
ＩＰヘッダチェック部
12
パケット
廃棄処理部
ゲートウェイ

【図３】



α：ＴＴＬ初期値
β：ＴＴＬ初期値－最大通過ｹﾞｰﾄｳｪｲ数